SCADA SYSTEM

CLASSIFICATION

Agenda

- Introduction
  - History
  - What is SCADA?
- Classifications of a SCADA system
  - Elements of SCADA system?
  - Where is SCADA used?
  - What types of SCADA are there?
- Purpose of this research
- Conclusion

Introduction

SCADA (Supervisory Control and Data Acquisition) System

- History
- Why SCADA?
- Definition of SCADA

History

- Egyptian supervisory
- First half of the 20th century
- Development from telemetry system
- Weather predictions
- Rail road tracks
- Two way system
- 1960s idea for supervisory
- 1970s radio system

Why SCADA?

- Saves Time and Money
  - Less traveling for workers (e.g. helicopter ride)
  - Reduces man-power needs
  - Increases production efficiency of a company
  - Cost effective for power systems
  - Saves energy
- Reliable
- Supervisory control over a particular system

What is SCADA?

- Supervisory Control and Data Acquisition
- Supervisory
  - Operator/s, engineer/s, supervisor/s, etc
- Control
  - Monitoring
  - Limited
  - Telemetry
  - Remote/Local
- Data acquisition
  - Access and acquire information or data from the equipment
  - Sends it to different sites through telemetry
  - Analog / Digital

Classifications

- Anatomy of a SCADA system?
  - Elements of SCADA
  - Levels of SCADA
- Where is SCADA used?
  - Different applications of SCADA systems?
- What types of SCADA are there?
- Component manufacturers and system manufacturers of the SCADA systems?
  - Automation Solutions
  - Software
  - Hardware

Elements of SCADA

Elements of a SCADA system

- Sensors and actuators
- RTUs/PLCs
- Communication
- MTU
  - Front End Processor
  - SCADA server
  - Historical/Redundant/Safety Server
  - HMI computer
  - HMI software

Sensors

Types of sensors:

- Pressure sensors
- Temperature sensors
- Light sensors
- Humidity sensors
- Wind speed sensors
- Water level sensors
- Distance sensors

Actuators

Actuators:

- Valves
- Pumps
- Motors

RTUs

RTU – Remote Terminal Unit

- Intelligent to control a process and multiple processes
- Data logging and alarm handling
- Expandable
- Asks the field devices for information
- Can control IEDs (Intelligent Electronic Device)
- Slave/Master device

Alarms

Types of alarms:

- Good alarms
- Critical failure alarms

Safety instrumented systems

Actions:

- Override the normal control system
- Take over the actuators

PLCs

PLC – Programmable Logic Controller

- Ladder logic
- Industrial computer that replaced relays
- Not a protocol converter
- Cannot control IEDs
- Communication compatibilities
- Takes actions based on its inputs

Communication

Communication systems:

- Switched Telephone Network
- Leased lines
- Private Network (LAN/RS-485)
- Internet
- Wireless Communication systems
  - Wireless LAN
  - Global System for Mobile Communication (GSM) Network
  - Radio modems

Communication cont.

Protocols:

- MODBUS
- DNP 3.0
- Fieldbus
- Controller Area Network (CAN)
- Profibus
- DirectNet
- TCP/IP
- Ethernet

Front End Processor

Front End Processor

- Gathers all communications and converts them into SCADA friendly communication
- Communication interface between several RTU channels and the host Master Station computer

SCADA server

SCADA Server

- It can be a Web server
- Data logging
- Analyzing data
- Serve the clients through a firewall
- Clients connected in the corporation or connected outside through internet
- Real-time decision maker
- Asks RTU for information

Historical server

Historical/Safety/Redundant Server

- Logs the data from the SCADA server and stores it as a backup, in case of a disaster
- It is basically a safety server

HMI Computer

Human Machine Interface Computer

- Access on the SCADA Server
- Control the system
- Operator Interface
- Software
  - User friendly
  - Programmable (C, C++)

DCS

DCS – Distributed Control System

- Process oriented – tendency to do something
- Not event oriented – does not depend on circumstances
- Local control over the devices
- Subordinate to SCADA

Levels of SCADA

Four levels of SCADA system

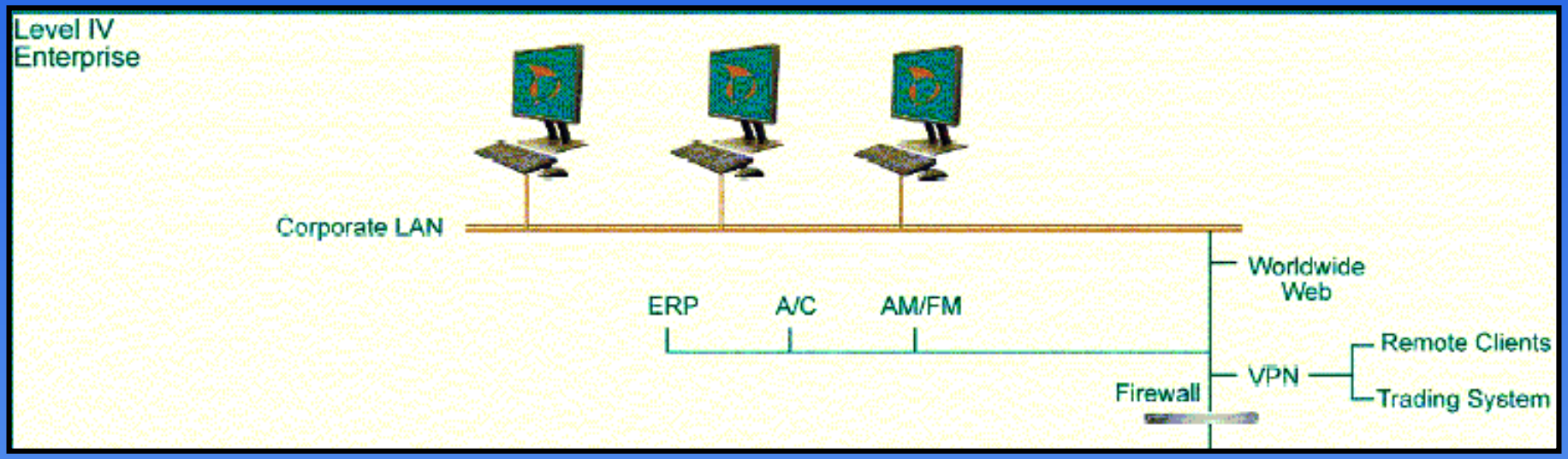
- Level IV - Enterprise
  - Corporate LAN/WAN
  - World Wide Web
  - Virtual Private Network
  - Firewall for remote users
- Level III – SCADA / MTU
  - Operator Workstations
  - Control
  - Engineering Workstations
  - Servers – Data logging

Levels of SCADA cont.

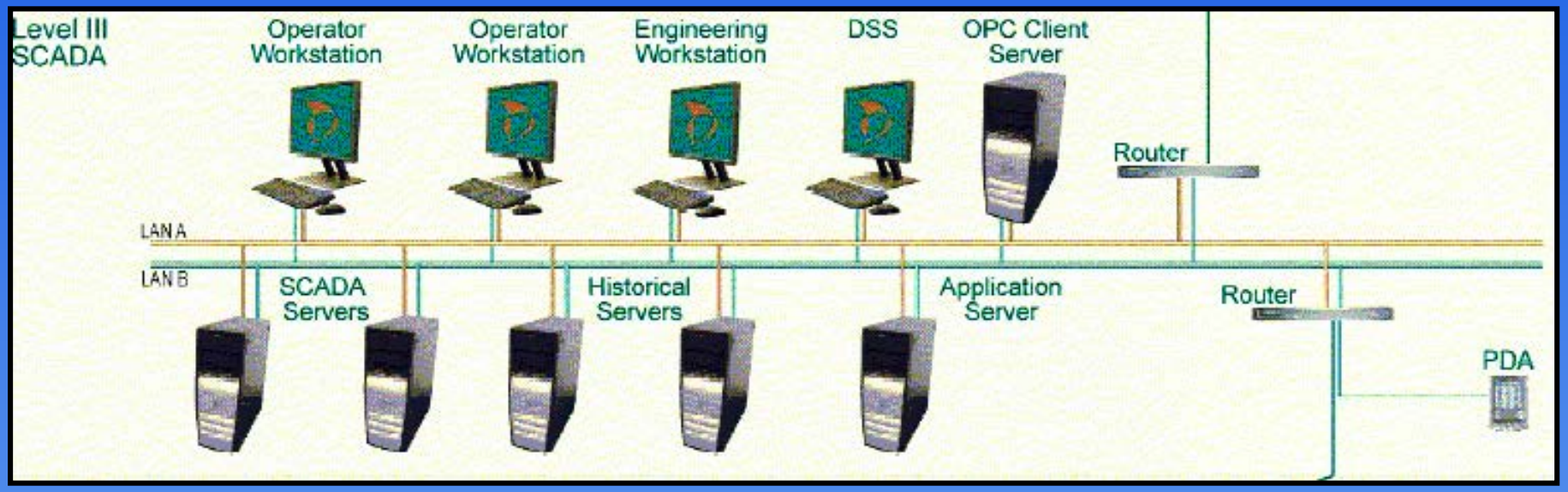
Four levels of SCADA system

- Level II – Telecommunication
  - Fiber
  - Radio
  - Telephone leased line
  - Protocols
- Level I – Field
  - Devices
  - RTUs / PLCs
  - Sensors

Level IV - Enterprise

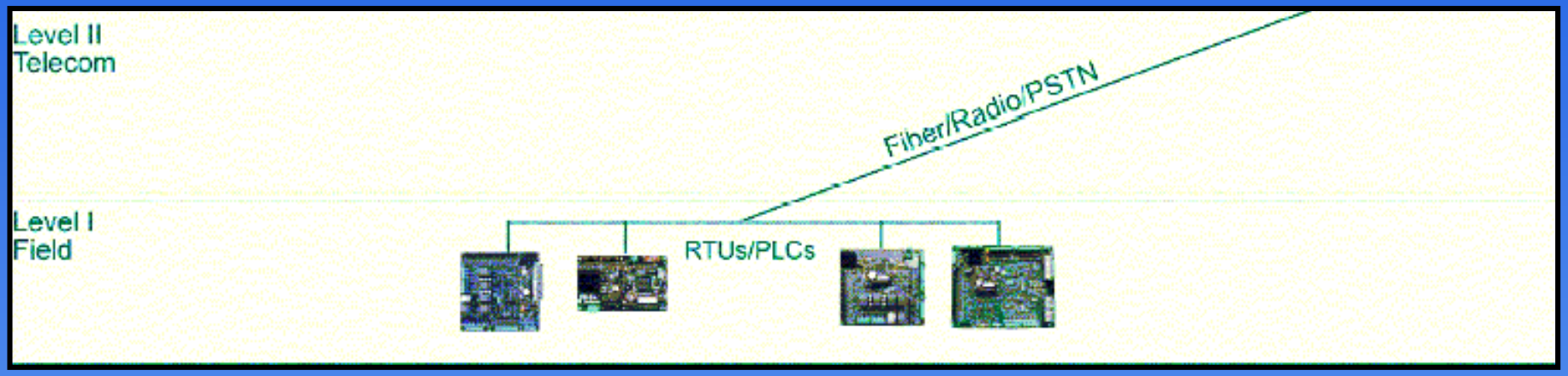


Level III - SCADA



Level II and I

Telecommunication and Field

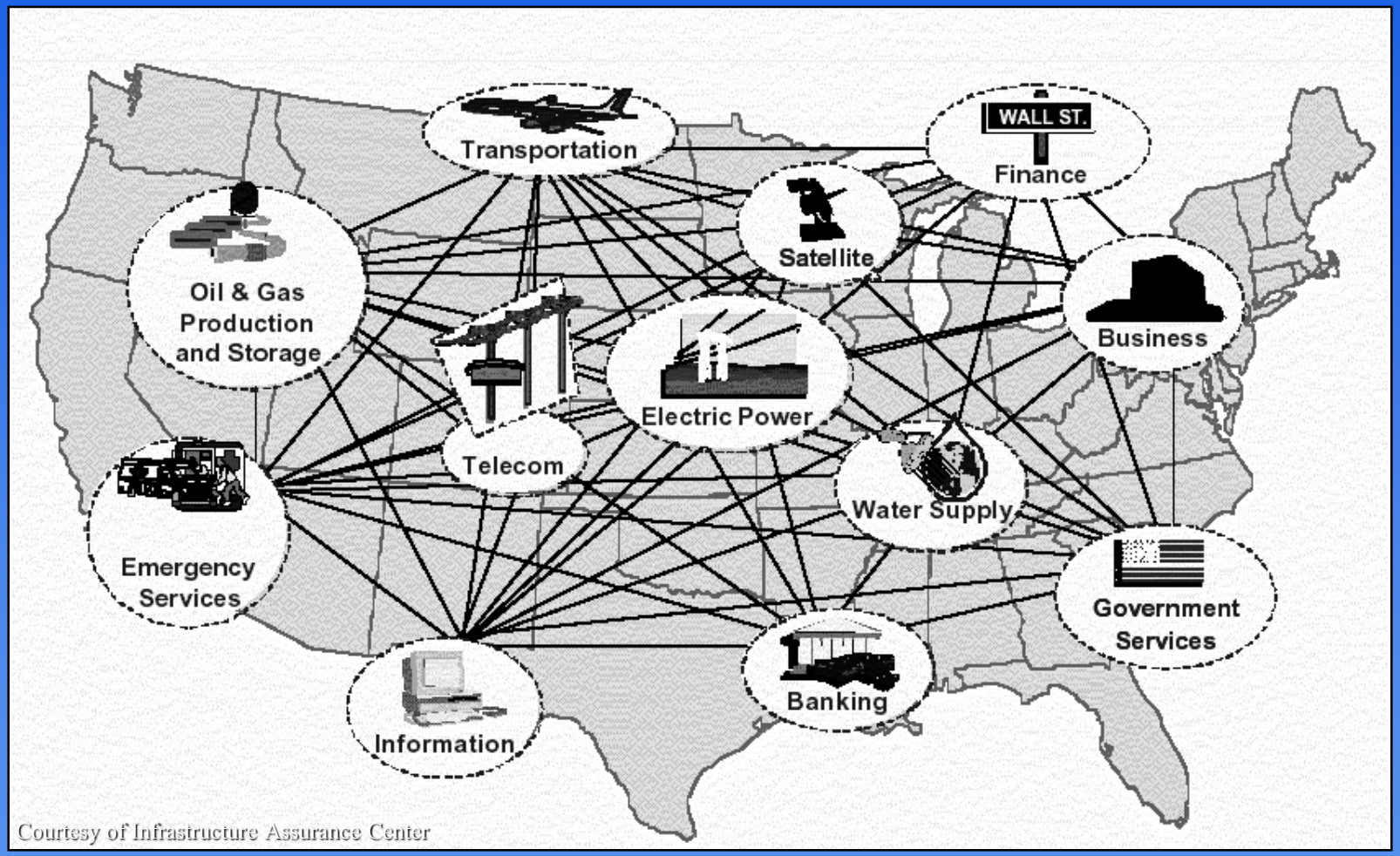


Where is SCADA used?

Main SCADA applications:

- Water and Wastewater
- Power
- Oil and Gas
- Research facilities
- Transportation
- Security systems
- Siren systems
- Irrigation
- Communication control

U.S. Infrastructure

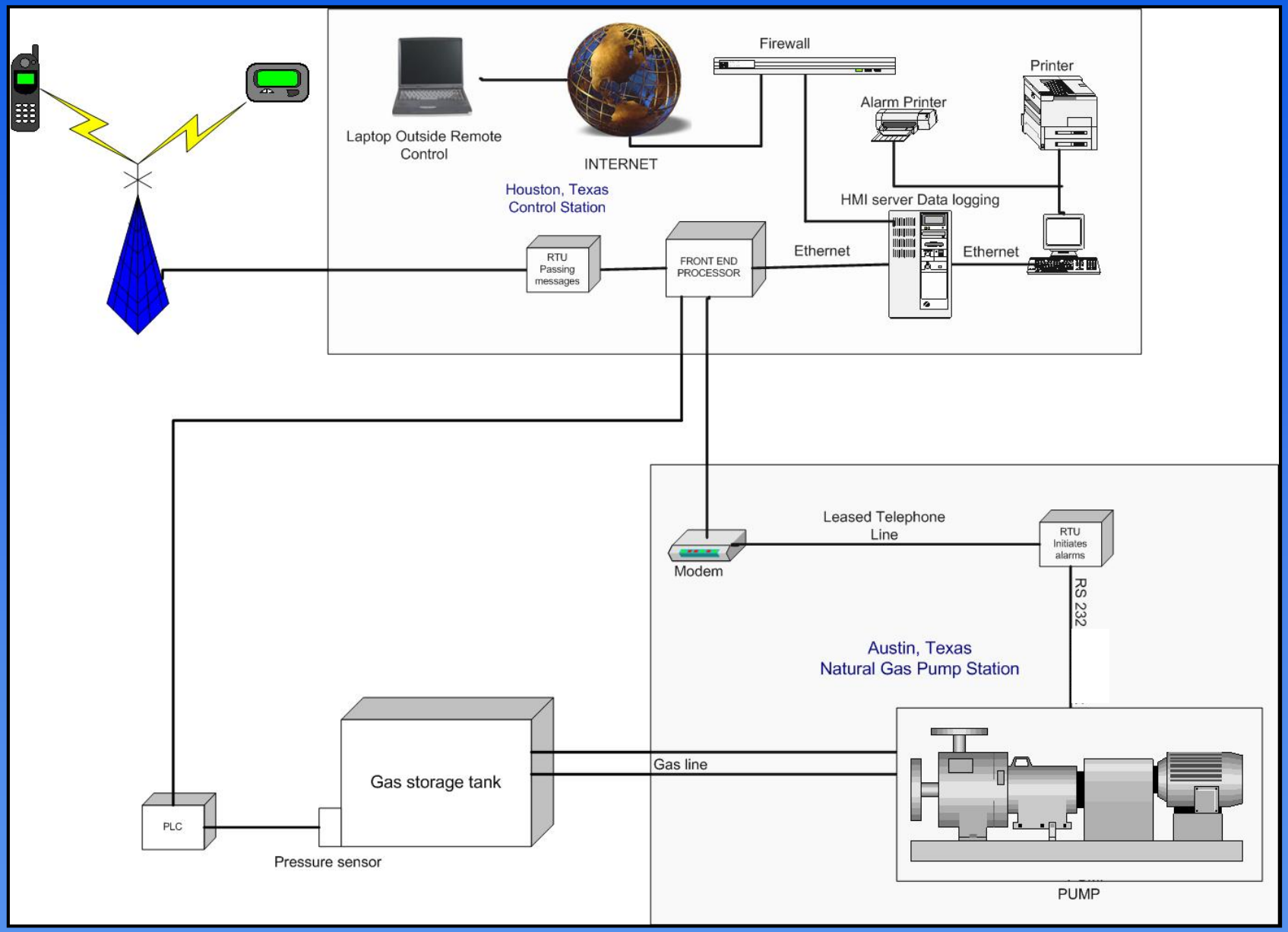


SCADA examples

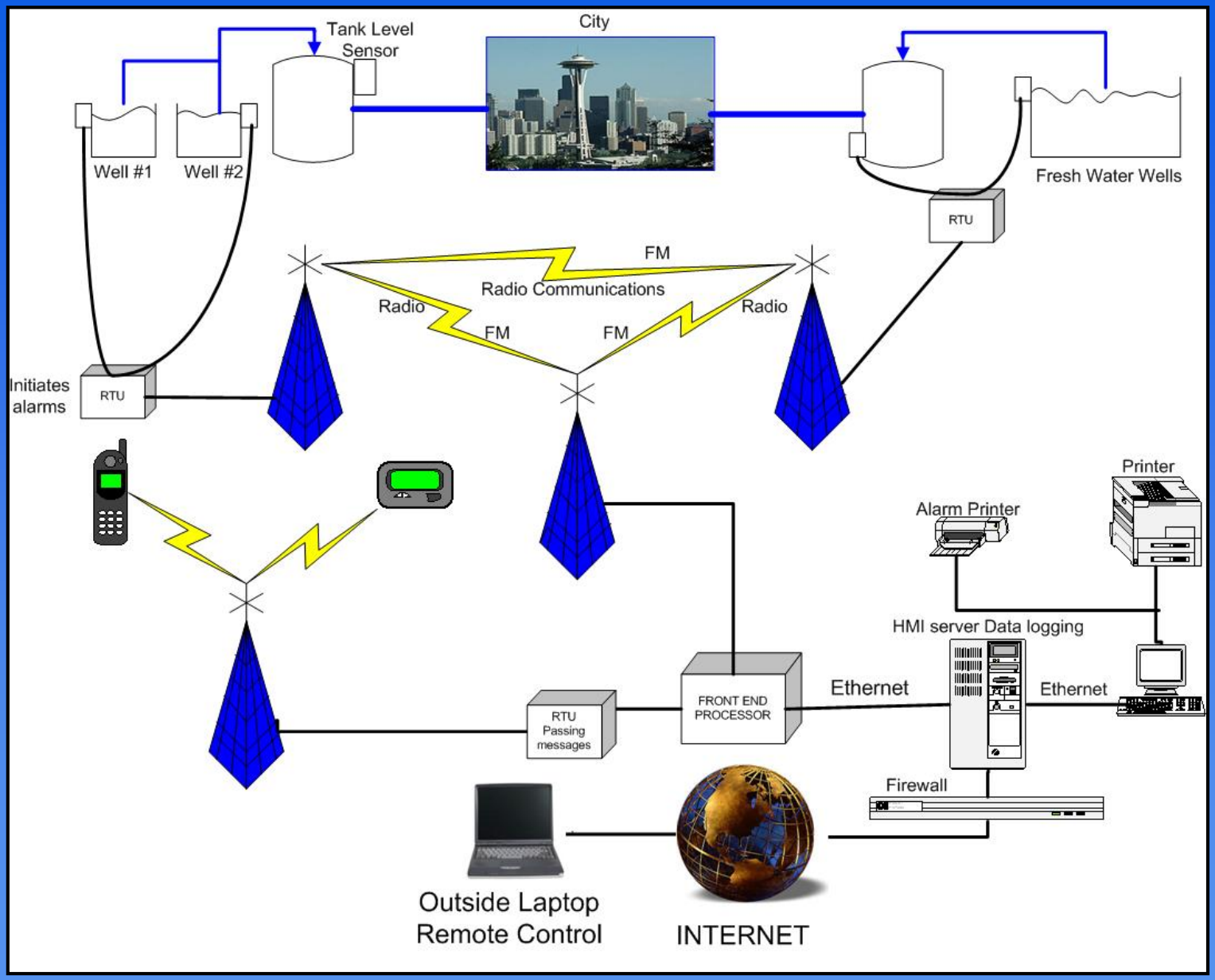
SCADA examples:

- Gas control systems
- Water control systems
- Power systems

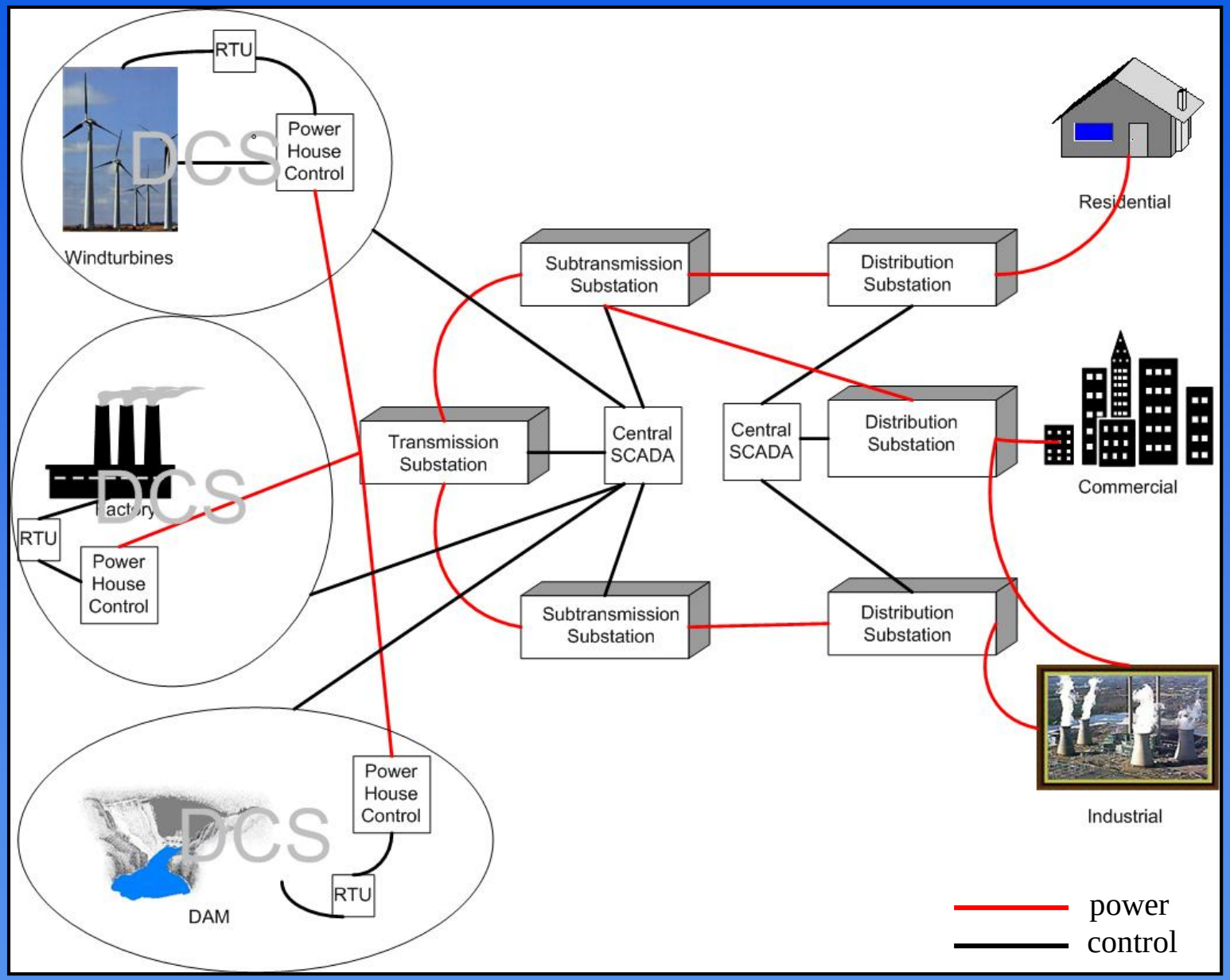
Gas SCADA


Laptop Outside Remote Control
INTERNET
Firewall
Printer
Alarm Printer
HMI server Data logging
Houston, Texas
Control Station
RTU Passing messages
FRONT END PROCESSOR
Ethernet
Ethernet
Leased Telephone Line
RTU Initiates alarms
Modem
RS 232
Austin, Texas
Natural Gas Pump Station
Gas storage tank
Gas line
PLC
Pressure sensor
PUMP

Water SCADA


Tank Level Sensor
City
Well #1
Well #2
Fresh Water Wells
RTU
FM
Radio Communications
Radio
FM
FM
Radio
Initiates alarms
RTU
Printer
Alarm Printer
HMI server Data logging
Ethernet
Ethernet
FRONT END PROCESSOR
RTU Passing messages
Firewall
Outside Laptop Remote Control
INTERNET

Power SCADA

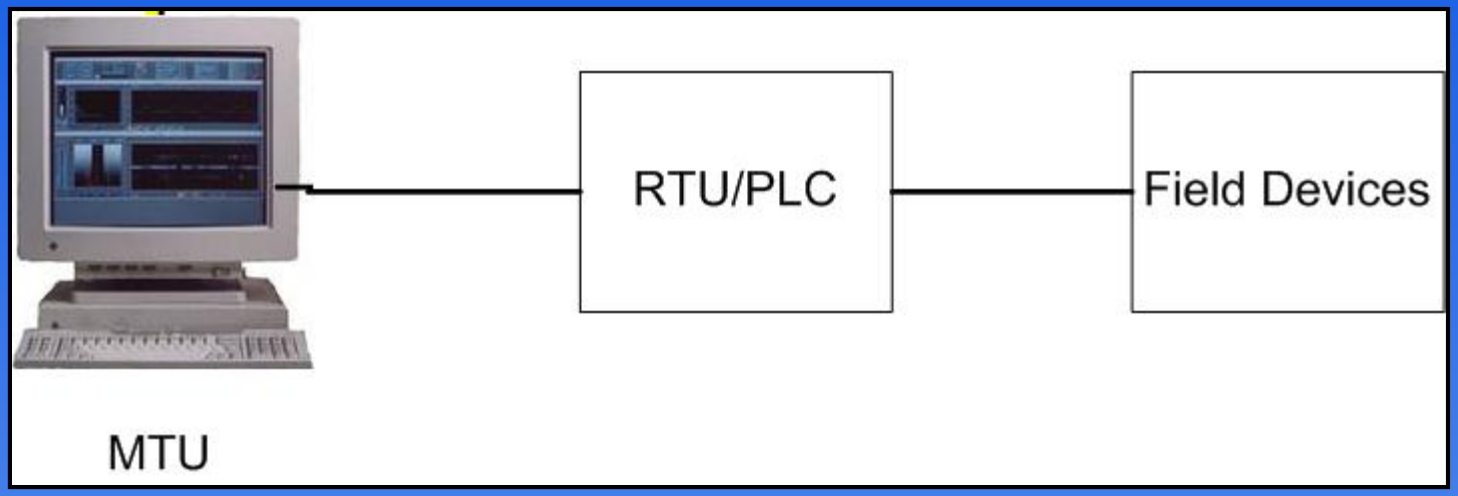

RTU
Power House Control
DCS
Windturbines
Residential
Subtransmission Substation
Distribution Substation
Transmission Substation
Central SCADA
Central SCADA
Distribution Substation
Commercial
RTU
Power House Control
DCS
Subtransmission Substation
Distribution Substation
Power House Control
DCS
RTU
DAM
Industrial
power
control

SCADA system types

Three types of basic SCADA systems:

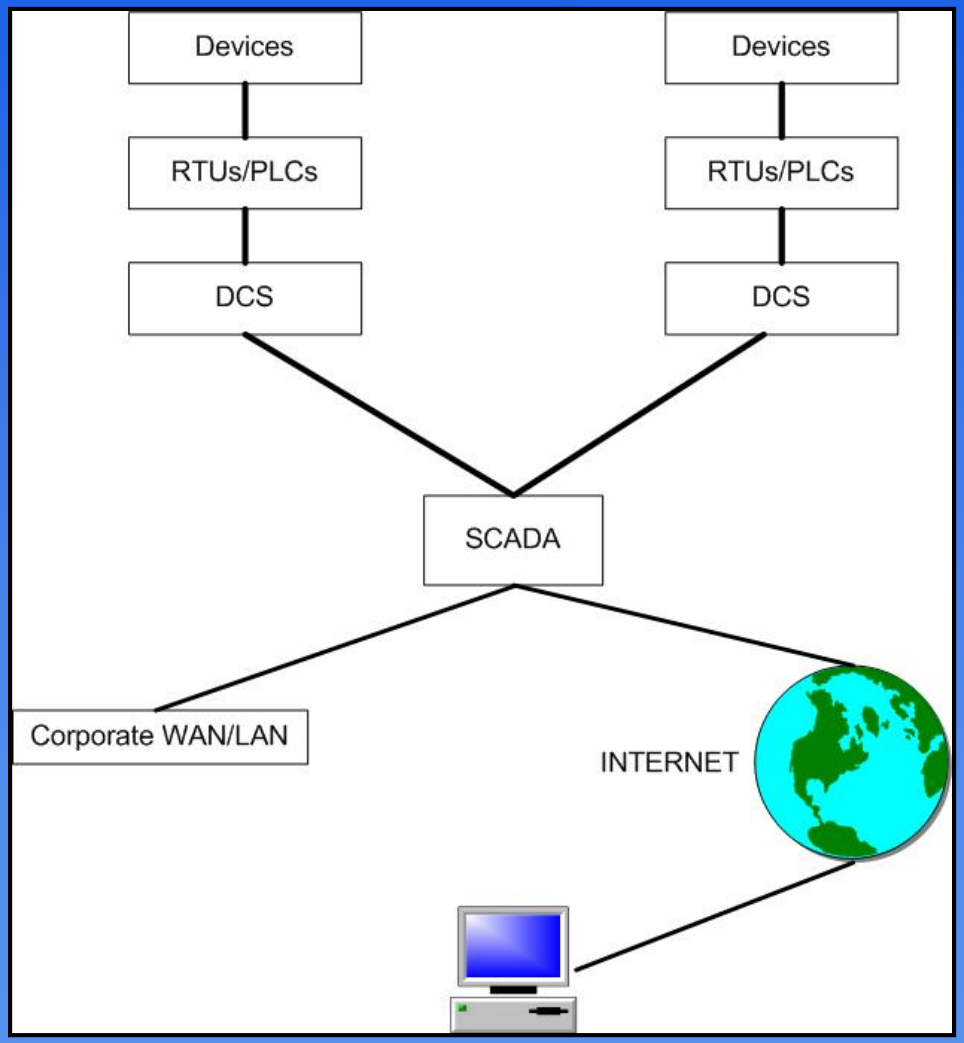
- Basic SCADA
  - One machine process
  - One RTU and MTU
- Integrated SCADA
  - Multiple RTUs
  - DCS
- Networked SCADA
  - Multiple SCADA

Basic SCADA



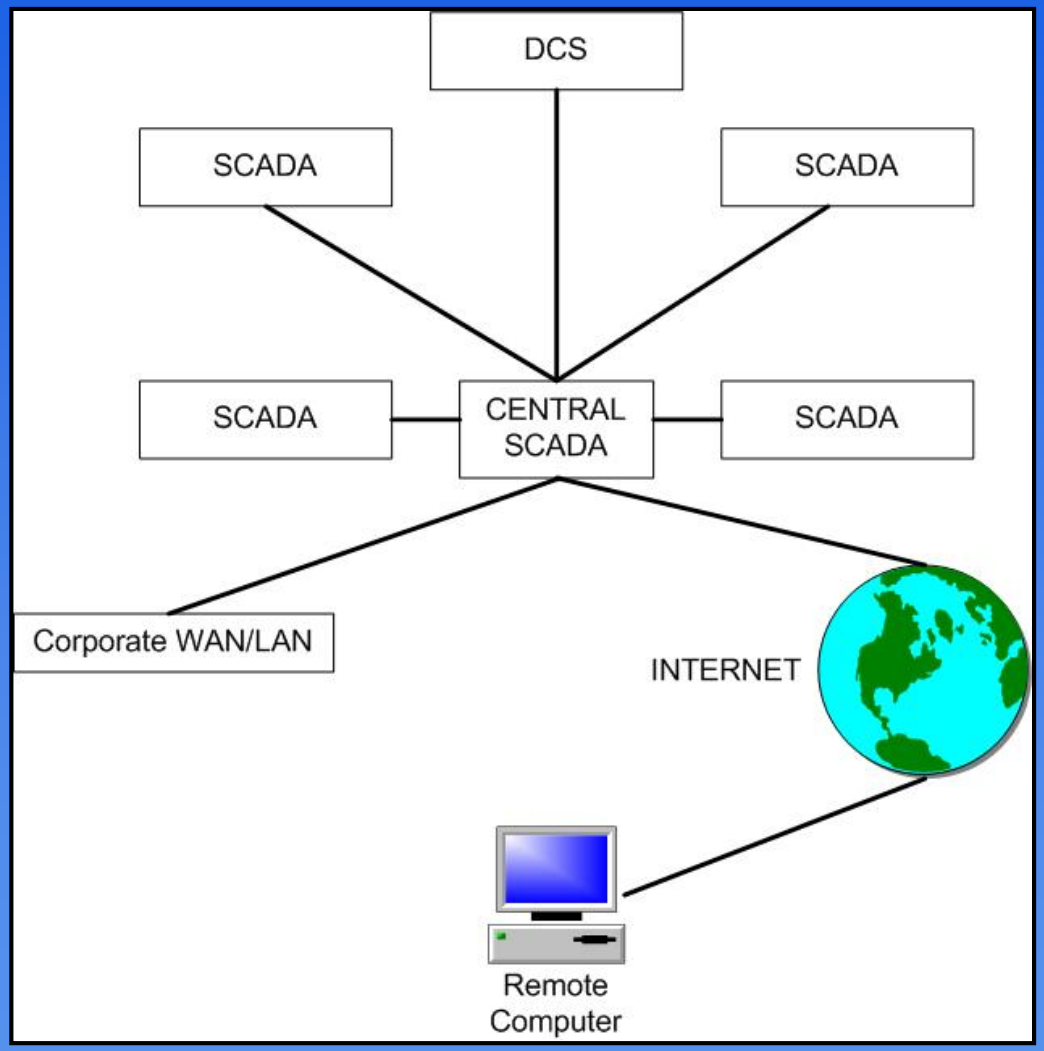
- Car manufacturing robot
- Room temperature control

Integrated SCADA



- Water systems
- Subway systems
- Security systems

Networked SCADA



- Power systems
- Communication systems

Automation solutions

SCADA system manufacturers

- Modular SCADA, UK
- MOSCAD, Motorola
- Rockwell Automation
- ABCO
- ABB
- Lantronix

SCADA Hardware

SCADA Hardware manufacturers

- Rockwell Allen Bradley
- General Electric (GE)
- Emerson
- Schneider Electric

SCADA Software

SCADA Software manufacturers

- Intellution (Fix 32)
- Iconics (Genesis32 v7.0)
- Wonderware (InTouch)
- Citect (CitectSCADA 5.42)
- National Instruments (Lookout SCADA)

Purpose of this research

- Develop a teaching module for a general SCADA system
- Develop a general model of a SCADA system
- Use LabView and wireless communication computers to illustrate an example of the SCADA system
- Study the vulnerabilities of the SCADA system
- Create a freshman introduction module
- Create an upper level course for SCADA

What is next?

- Use the Laptop1 to generate the wells, tanks, servers, RTUs PLCs and the front end processor through SubVIs
- Use the Laptop2 to be the HMI Computer that connects to Laptop1 and reads the data and also affect the devices
- And Laptop3 to simulate an attack at the SCADA system

Conclusion

- There are thousands of SCADA systems installed and they can be completely different from each other, in terms of their structures but they all have common elements and a common purpose – to supervise control and collect data.

- There are three types of SCADA systems that describe all of the SCADA systems.

- Communication is the most significant part of SCADA

- Power and communication systems are most likely to get attacked by terrorists.

Discussion